Source Brief

Enterprise Infrastructure Security Solutions based on Intel® Architecture

Delivering Dynamic Security Protection With Agile and Adaptive Solutions

The downside can be huge. Failing to stay a step ahead of hackers can result in damage ranging from the slightly inconvenient to the utterly catastrophic. IT professionals are in a race against more sophisticated threats and increasing network traffic. Many attacks are masquerading as legitimate application layer traffic and getting past traditional firewall-based security appliances that focus on network layer access. "The antivirus market will continue to lead the security software market in 2007, but because of changing threats, there is a long-term technology shift away from complete reliance on signature-based antivirus defenses to more-predictive proactive defenses," says Nicole Latimer-Livingston, principal research analyst at Gartner[1].

Security attacks are becoming more dynamic, which necessitates deeper packet inspection and preventative strategies across all network layers. These attacks target the application layer and expose corporate assets that are stored in software applications such as financial, ERP and CRM. However, companies that choose to lock down their networks may do so at the expense of users who expect a high level of performance. Helping to minimize trade-offs between adaptive security and performance, Intel and other industry players are developing solutions that address the needs of small, medium and large enterprises. These solutions can utilize the latest technologies to safeguard networks running at speeds in excess of 40 gigabit per second (Gbps).

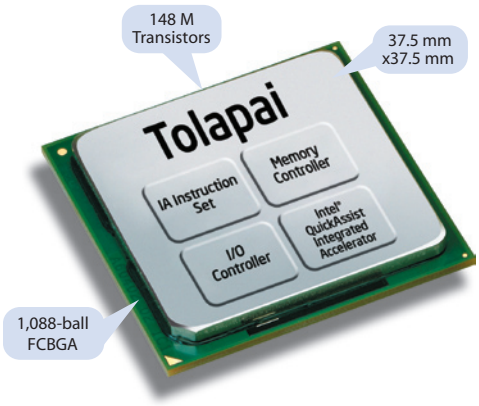


Figure 1. Single-chip security solution

Security Trends

Many cybercriminals, motivated by monetary gain instead of intellectual rewards, seem to be more interested in stealing and exploiting confidential data than bringing down a whole system. They are breaking into web-based applications and accessing valuable data such as customer and transaction information as well as other proprietary corporate data. This is just one example of an application-layer attack that can easily penetrate many conventional network perimeter security schemes. In its *Internet Security Threat Report, Trends for January–June 07,* Symantec reported 61 percent of the vulnerabilities disclosed during the first half of 2007 affected Web applications.[2,3]

Another trend is the diminished preoccupation of protecting "the edge of the network" and moving the focus inward, by placing security appliances between one or more internal subnets. Security is now about controlling the content of the network, not just the connections within a network. This transition is addressing one of the biggest risks to the enterprise, targeted attacks which can originate from either external (Internet) or internal (intranet) sources.

Whereas perimeter security appliances mostly monitor inbound traffic from the untrusted network, intra-network appliances must monitor traffic in two directions, which doubles the inspection duties. And typically, traffic within the enterprise flows at higher line rates than at the perimeter, one to ten gigabits per link as opposed to several hundreds of megabits.

Future-Proofing Security

The true value of a security system is its ability to deal with threats that have not yet appeared. Defending against future attacks requires security solutions that quickly update security policies and monitoring strategies. However, many traditional security devices are based on closed architecture and rely on hardware accelerators, like ASICs and FPGAs, to handle specific tasks very fast. After their initial configuration, ASIC or FPGA-based systems cannot be reprogrammed to address new attacks. This approach, with security applications hard-coded in custom chips, can be poorly equipped to respond to dynamic threats.

To address new threats, systems often include a general-purpose (GP) processor that can close these security holes through software updates. Solutions based on high-performance GP multi-core processors are extremely flexible and can handle new situations with predictable performance. These open systems adapt quickly to new security challenges, which allows them to maintain and even increase their value to the network over the long run.

Specialized Solutions for Small and Medium Businesses

Unfortunately for smaller companies, the task of securing networks does not seem proportional to the number of employees. Large and small businesses face similar challenges and need to protect themselves against Internet-based threats and employee devices, such as laptops and PDAs, that can spread viruses and malware when connected to the network. Small and medium businesses (SMBs) typically look for simplified security solutions offering automated, all-in-one service. They prefer one solution that blocks viruses, spyware, spam, phishing and hacker attacks and identifies thieves who breach PCs, servers and e-mail.

Helping security appliance makers cram all this functionality into one box, Intel developed a single chip, codenamed "Tolapai," shown in Figure 1. Due to arrive in mid-2008, Tolapai, combined with Intel® QuickAssist Technology, integrates an Intel® Architecture core, memory controller and I/O controller, and is optimized for small form factor security appliances. The high-performance CPU core supplies the horse power needed to perform deep packet inspection and other complex operations.

Since many security vendors already incorporate Intel® processors, they can run existing software applications on Tolapai because it is backward code compatible with earlier Intel processors. Intel QuickAssist Technology provides security acceleration for processing standard functions, such as bulk encryption, running at 1.6 Gbps line rates. This combination delivers performance without sacrificing the programmability required to respond to dynamic threats.

Tolapai supports a broad range of applications, including communications and security processing, while remaining cost-effective and power-efficient. In many cases, security appliance designers can forgo specialized co-processors and dedicated security hardware, which can decrease board size by about 45 percent while reducing power consumption by almost 20 percent.

Multi-Core Processors Boost Performance for Large Enterprises

Several networking trends are pushing the limits of security infrastructure in large enterprises. Networks are transitioning to 10 gigabit Ethernet and need faster I/O to keep up with greater network traffic. Threats are more sophisticated and content-based, so security solutions must perform deeper

inspections of packets, faster than ever before. In addition, many enterprises are deploying security devices to safeguard the intranet – traffic within the company – which typically carries more traffic than Internet connections.

With its expertise in multi-core processors, Intel is engaged with many of the industry leaders developing security hardware and software solutions based on leading-edge technologies. These solutions include high-end security appliances, such as the Nokia IP2450* security platform, that are designed for the demanding price-performance and multi-gigabit Ethernet throughput requirements of large businesses and service providers.

Power-Efficient Multi-Core Processors

Many of these leading-edge platforms are equipped with two Quad-Core Intel® Xeon® processors 5300[Δ] series, a total of eight CPU cores, which supply the performance headroom needed to meet today's and tomorrow's security challenges. Based on the Intel® Core™ microarchitecture, these processors offer break-through performance: up to three times the raw performance and performance/watt[4] of previous-generation single-core processors. This translates into greater performance with fewer cooling challenges and enables security applications to run within a smaller footprint.

Multi-Core Optimized Security Software

Intel is highly engaged with the independent software vendor (ISV) community and other software developers to provide tools and expertise for optimizing software for multi-core platforms. Vendors like Check Point Software Technologies have announced products (e.g., CoreXL*) to fully utilize the performance offered by GP multi-core processors. Some of the techniques may involve: sharing security inspection duties throughout all cores; using advanced load balancing to increase throughput; and partitioning security functions across multiple cores. CoreXL is a Check Point product and is not a member of the Intel® Core™ processor family.

Software optimizations have a significant impact on the overall performance of the system. For instance, Check Point observed a 600 percent throughput increase when CoreXL is activated[4]. On a reference system using two 2.66 GHz Quad-Core Intel Xeon processors 5300 series, the throughput was raised from 300 Mbps to more than 1.8 Gbps[4].

Security-Hardened, High-Performance Security Appliances

A critical requirement for many of today's computing environments is power efficiency and throughput. Intel QuickAssist Technology comprises a number of initiatives that support accelerator innovation for a variety of applications, including network security. GP computers allow programmers to implement virtually any algorithm in software. However, even with today's fastest multi-core processors, there are still many algorithms that can-

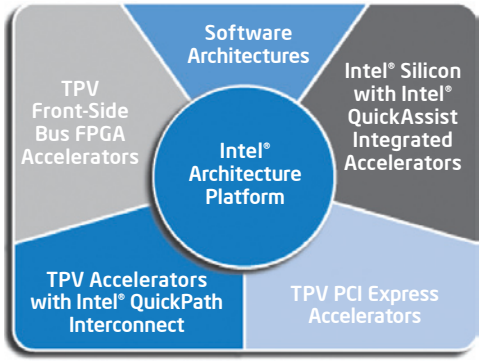


Figure 2. Intel® QuickAssist Technology is a comprehensive initiative that consists of interrelated Intel and industry-standard technologies that enable accelerators on Intel® platforms.

not execute fast enough to meet some customer requirements. Appropriately partitioning a problem between a CPU and one or more accelerators permits applications to execute dramatically faster.

Intel is looking for ways to make the development process easier for developers while enabling better end-products. Intel QuickAssist Technology addresses both by promoting innovation in accelerators equating to:

- **Decreased development time.** Independent software vendors no longer need to develop proprietary acceleration layers for each new device.
- **Increased business flexibility.** End-users can choose devices and solutions that fit their changing business requirements without being tied to a particular accelerator.
- **Future ready.** Built to last through future generations of multi-core processor designs.

Comprehensive Security Software Module

Another large enterprise security solution that employs multi-core processors is the iGateway* Firewall from Intoto. They are a leading provider of security software for network infrastructure equipment offering a comprehensive security software module that supports 16 Gbps line rates. "We have leveraged general-purpose multi-core processors very effectively to deliver the performance often found only in higher cost ASIC-based solutions. With this offering, OEMs can meet customers' stringent performance demands on their infrastructure equipment while reducing their development costs," says Sathyan Iyengar, president and CEO, Intoto.

Telecom and networking equipment manufacturers looking to accelerate their time-to-market can integrate an embedded security software module designed to protect networks from external and internal threats. The Intoto iGateway Firewall provides stateful packet inspection, content filtering and protection at 16 Gbps line rates.

Security Consolidation Lowers Cost For Large Enterprises

Just as server consolidation is driving down cost and footprint for data centers, security applications are being consolidated onto high-end network security platforms. This eliminates the cost of maintaining multiple traditional point security products, dramatically driving down the total cost of ownership and stopping appliance sprawl.

As the demand for bandwidth increases, adoption of 10 Gbps Ethernet is on the rise. This is creating a demand for security appliances that need to keep up with line rates over 20 Gbps. For instance the X-Series* of platforms from Crossbeam Systems enable enterprises to consolidate their best-of-breed security applications onto a purpose-built, highly available infrastructure. This chassis-based network security solution covers all of the major network security categories from firewall through web application protection. Based on the Intel Quad-Core Intel Xeon processors, this platform has the ability to run more than 1500 virtual firewalls in a single system, and this combination can yield a fast and compelling return on investment (ROI).

New Technologies Help Protect IT Investment

Technology leaders are working together to develop next-generation security systems that address the challenges of dynamic and more sophisticated security threats. These systems are based on general-purpose multi-core processors that are easy to program and can handle new situations with predictable performance. Moreover, Intel's product roadmaps and flexible technologies are helping security equipment makers protect their development investments. Using these innovations, security vendors are developing families of security products with common building blocks and reducing cost through the powerful combination of high-performance processors and code compatibility.

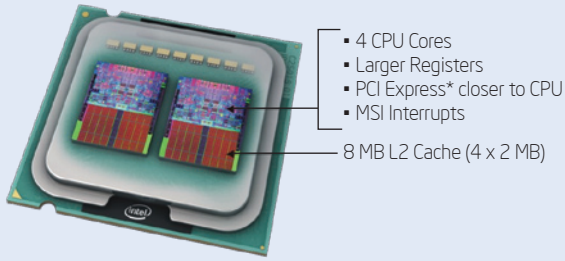
To learn more about technologies that help preserve the value of security solutions, please visit http://www.intel.com/netcomms/technologies/security/index.htm

Benefits of Intel® Multi-Core Processors in Security

The latest multi-core processors from Intel are delivering the security performance that previously required specialized hardware and processors. Here are some Intel® Architecture features that enhance security processing:

- Many more CPU cores in the system
  - Increase compute capacity within the same power envelope
  - Process more TCP flows simultaneously
- Larger internal registers (128 bits)
  - Execute pattern matching (virus detection) faster
- PCI Express* bus interfaces closer to the CPU
  - Decrease the time to process network traffic (lower I/O latency)
- Large on-chip memory caches
  - Decrease the time to perform deep packet inspection

In addition to these architecture advantages, equipment makers typically find maintaining software code for general-purpose processors, like the Quad-Core Intel® Xeon® processor 5300 series, is easier than for application-specific hardware. This is because Intel® processors are supported by a broad ecosystem offering a wide range of mature development tools.



The Quad-Core Intel® Xeon® processor 5300 series

[Δ] Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

[1] "Gartner Says Worldwide Security Software Revenue Will Reach $9.1 Billion in 2007," Gartner, Inc., Feb. 1, 2007. http://www.gartner.com/it/page.jsp?id=500694 This document is for informational purposes only. Intel makes no warranties, express or implied, in this document.

[2] Vulnerabilities are design or implementation errors in information systems that can compromise the confidentiality, integrity or availability of information.

[3] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf.

[4] Performance tests and ratings are measured using specific computer systems and/or components and reflect approximate performance of Intel® products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit http://www.intel.com/performance/resources/benchmark_limitations.htm

Printed in USA 0208/MS/OCG/XX/PDF ♻ Please Recycle 319338-001US